

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MISC. 12 -033

-----X
IN THE MATTER OF AN APPLICATION
OF THE UNITED STATES OF AMERICA
FOR ORDERS AUTHORIZING THE
DISCLOSURE OF LOCATION DATA
RELATING TO TWO SPECIFIED
WIRELESS TELEPHONES

FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF
APPLICATION

(Fed. R. Crim. P. 41 and
57(b); T. 18, U.S.C.,
§§ 3103a and 3117;
T. 28, U.S.C., § 1651(a))

-----X
EASTERN DISTRICT OF NEW YORK, SS:

I, Sean Olsewski, being first duly sworn, hereby depose
and state as follows:

1. I make this affidavit in support of an application
for search warrants under Federal Rule of Criminal Procedure 41
and 18 U.S.C. §§ 2703(c)(1)(A), 3103a and 3117, for information
about the location of the cellular telephones assigned numbers
(1) (714) 348-6972, a cellular telephone subscribed to by "Doki
Lungo" of the listed address "El Vido Way 45 23, Orange, CA"
("Subject Telephone #1"); and (2) (714) 253-2922, a prepaid
cellular telephone with no subscriber information, but a listed
address of 17330 Preston Road, Dallas, TX 75252 ("Subject
Telephone #2") (collectively, the "Subject Telephones"), whose
wireless telephone service providers are Sprint Nextel and AT&T,
respectively (collectively, the "Service Providers"). The
Subject Telephones are described herein and in Attachment A, and
the location information to be seized is described herein and in
Attachment B.

2. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for approximately nine years, and I am presently assigned to Squad C-42, which is responsible for investigating emerging organized criminal groups. Accordingly, I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups engaged in international organized criminal activity, such as international fraud and identity theft schemes. My experience includes nearly seven years conducting counterintelligence investigations, which are often conducted in coordination with other law enforcement agents, including foreign investigating agencies and fellow law enforcement agents based in the United States. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their identities and activities from detection by law enforcement authorities.

3. The facts in this affidavit come from my personal observations, my training and experience, information obtained from other agents, including law enforcement agents in Germany, and my review of text messages and draft transcripts of cellular telephone calls intercepted by German law enforcement authorities. Because the purpose of this affidavit is limited to demonstrating probable cause for the requested warrants, it does not set forth all of my knowledge about this matter. Summaries

of intercepted telephone calls are based on draft transcripts and draft translations, which are subject to revision. In addition, when I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that a European-based organized criminal group is involved, together with participants in the United States, in a conspiracy and fraud scheme involving the theft and use of stolen credit- and debit-card information, in violation of 18 U.S.C. §§ 1028A and 1029(a) & (b) (the "Subject Offenses"). Based on the information I have learned regarding the fraud scheme to date, there is also probable cause to believe that the Subject Telephones are being used to commit the Subject Offenses, in that they are being used to communicate internationally in furtherance of the fraud scheme. There is therefore probable cause to believe that information regarding the Subject Telephones, including the location information described in Attachment B, will constitute evidence of the Subject Offenses, and will lead to the identification of individuals in possession of the Subject Telephones who are engaged in the commission of those offenses.

PROBABLE CAUSE

5. There is probable cause to believe that the individuals utilizing the Subject Telephones are involved in an

organized international fraud scheme. Specifically, there is probable cause to conclude that certain telephone calls to and from the Subject Telephones that have been intercepted by German law enforcement authorities constitute communications with U.S.-based participants in the fraud conspiracy concerning the status of the conspiracy and how the fraud is being effected, as set forth below.

a. I have been advised that German law enforcement authorities are engaged in an investigation of European-based groups engaged in the international fraud scheme detailed herein. During the course of the German investigation, which utilized wiretaps, telephone calls and text messages to and from the Subject Telephones were intercepted.

b. In this case, based on the information gathered to date, the evidence shows that individuals in Germany, working together with others in Romania, the United States, Mexico, Thailand and Malaysia, are involved in a scheme to steal credit and debit card information from unsuspecting targets in Germany. According to German law enforcement authorities, the scheme involves burglarizing dozens of home-improvement stores and grocery stores in Germany - or surreptitiously staying behind in those stores after closing - in order to install hidden storage devices in the "point-of-sale" ("POS") credit- and debit-card terminals at the stores' checkout counters. Those stroage

devices, in turn, capture credit- and debit-card account numbers, and PIN codes, from shoppers at the stores, and transmit that information wirelessly to cellular telephones used by the conspirators. Fraudulent credit- and debit-cards manufactured using those stolen account numbers and codes have subsequently been used to make unauthorized cash withdrawals from automated teller machines in the New York area, including machines located in Queens, Nassau County, and Manhattan, as well as in Mexico, Thailand and Malaysia.

c. I have reviewed surveillance images from security cameras at branches of J.P. Morgan Chase bank in Queens, Nassau County, and Manhattan. Those images show several individuals, whose identities have not yet been determined, making cash withdrawals using account information and pin codes that were stolen from victims in Germany pursuant to the above-described scheme.

d. German law enforcement authorities have identified a Romanian national, CORNEL-ADRIAN CONSTANTIN ("CONSTANTIN"), whom they believe to be involved in above-described conspiracy. I have reviewed draft translations of draft transcripts of a series of telephone calls between numbers associated with CONSTANTIN in Germany and Subject Telephone #2 between November 14, 2011 and November 15, 2011, and between numbers associated with CONSTANTIN and Subject Telephone #1

between November 22, 2011 and November 28, 2011. Based on my training and experience, and conversations with fellow law enforcement agents, I understand CONSTANTIN, speaking in Romanian, to be using coded language to update one or more New York-based co-conspirators on the status of the conspiracy and how the fraud is being effected.

Subject Telephone #2

e. For example, on or about November 14, 2011, at approximately 10:18 a.m. EST, the following conversation occurred between an individual identified by German law enforcement agents as CONSTANTIN and an unidentified male ("UM") using Subject Telephone #2:

CONSTANTIN: Can you hear me?

UM: Yes, I think you're not getting a tone.

CONSTANTIN: No, no, I was just scared, I thought my phone was being intercepted.

UM: That can't be, you haven't done anything . . . or have you done anything you need to worry about?

CONSTANTIN: No, brother, I haven't done anything. I've been working hard to get it done, but I haven't pulled it off.

UM: Heh, but what have you done with the crew from Moldavia? Have you met with them?

CONSTANTIN: No, haven't done anything yet. They called me at night and said I need to get myself prepared. When I called them on Sunday, they didn't answer. All the phones were out of service.

UM: And they didn't call you back?

CONSTANTIN: No, nothing.

UM: That means that they have done or will do something else.

CONSTANTIN: I don't give a shit. I'm glad to be going home. They didn't bring me the stuff until Monday, damn it. Now I have to go home and do the installation work.

UM: What have you done? Did the package arrive from home?

CONSTANTIN: Yeah, that was shit too. They should have come on Sunday, but called and said their van broke down in Hamburg but that they would come early Monday morning.

UM: Good, good.

CONSTANTIN: Yeah, if there would have been a problem, I would have flipped out. I'm already close to it.

UM: Crazy shit man.

CONSTANTIN: Yeah, now all I have to do is get the installation done.

UM: Yeah, we didn't want to cause any problems.

CONSTANTIN: When I'm done, we'll do our thing. I'm working on it. When I'm done, we'll see.

UM: [How] will we handle it? You call me or me you?

CONSTANTIN: I'll call, it's going to take a while. I still have to download, polish up, etcetera. How about getting me the money in the meantime, please, okay?

UM: Yeah, I'll try to get it done today.

CONSTANTIN: Please try. I need money here now, and then we can talk. When I'm ready, I'll call.

UM: He brought that yesterday. I'll send it to you today.

CONSTANTIN: Good, brother.

Based on my training and experience and conversations with fellow law enforcement agents, I believe this conversation concerns preparations to manipulate point-of-sale credit- and debit-card terminals by installing electronic devices to steal account information. I believe CONSTANTIN's statement "I was just scared, I thought my phone was being intercepted," to refer to his concern about law enforcement monitoring of his illegal activities. I further believe his reference to the "Moldavia crew" to refer to several of his co-conspirators, who I believe are tasked with breaking into retail stores, or staying behind after the stores close, to manipulate the point-of-sale terminals, while his references to getting himself "prepared" and

doing the "installation work," refer to related technical tasks that are his own responsibility.

f. Information obtained from AT&T indicates that Subject Telephone #2 received calls from Romania at least as recently as November 23, 2011, and from Germany at least as recently as November 16, 2011.

Subject Telephone #1

g. On or about November 22, 2011, at approximately 12:15 p.m. EST, the following conversation occurred between an individual identified by German law enforcement agents as CONSTANTIN and an unidentified male ("UM") using Subject Telephone #1:

CONSTANTIN: Hello, man.

UM: What are you doing, taking a walk?

CONSTANTIN: Yeah, walking, driving. I'm going to meet them, 'cause they called me and said, "We're definitely doing something tonight."

UM: Take a kilo of meat with you, to distract them.

CONSTANTIN: Yeah, then I can grill something for them.

UM: Good, I thought you'd talk with them when you go by there. I spoke with them and they said that you'd surely be there Sunday morning.

CONSTANTIN: I'm not taking anything. I told you I was going home. I'm not staying.

UM: Yeah, I left you a message. On Sunday you still need to handle something.

CONSTANTIN: What kind of message did you leave me? I only read, "Hey, get me the gold." That's not a message.

UM: No man, I sent you a message. That means you may not have received it.

CONSTANTIN: I swear, I didn't get anything else. Damn it, today is Tuesday. I was ready to go.

UM: I told you, you'll surely be done on Sunday, have handled everything.

CONSTANTIN: What, they can't come any earlier?

UM: No, they can't.

CONSTANTIN: OK, until then.

Based on my training and experience, and information provided by German law enforcement agents, I believe that CONSTANTIN's statement "We're definitely doing something tonight," was a reference to a plan to manipulate point-of-sale terminals by installing electronic devices to steal account information. Indeed, German law enforcement agents conducting visual surveillance of CONSTANTIN on or about November 22, 2011, observed him drive from his residence in Hannover, Germany, to

Duisberg, Germany, where he was observed meeting with two co-conspirators who, the same night, were subsequently observed attempting to manipulate a point of sale device in a local home improvement store.

h. On or about November 25, 2011, at approximately 9:59 p.m. EST, the following text message was transmitted from Subject Telephone #1 to a cellular telephone that German law enforcement agents have indicated is used by CONSTANTIN:

Code: 42230502 you are to receive 717.31 Euro from RAUL CABA, NY

According to information obtained from Sprint Nextel, Subject Telephone #1 was in the vicinity of a cellular telephone tower in Long Island City, Queens at the time this text message was transmitted. I am informed by German law enforcement agents that CONSTANTIN subsequently received a Moneygram wire transfer in the amount of 717.31 Euros.

i. Information obtained from Sprint Nextel indicates that Subject Telephone #1 continued to be in active use until at least as recently as January 7, 2012.

6. Based on the foregoing, there is probable cause to believe that the individuals in possession of the Subject Telephones are engaged in an international scheme to defraud and commit identity theft, and that the Subject Telephones are being used in furtherance of the scheme, in that the coconspirators

appear to be using the phones to transmit information to coconspirators overseas, and to receive information from those coconspirators, regarding the status of the conspiracy and its operational details. There is thus probable cause to believe that the location information for the Subject Telephones, which will assist in identifying the individuals in possession of the Subject Telephones, constitutes evidence of criminal activity, including but not limited to conspiracy to commit access device fraud, in violation of 18 U.S.C. §§ 1029(a) and (b), and aggravated identity theft, in violation of 18 U.S.C. § 1028A.

7. In my training and experience, I have learned that the Service Providers are companies that provide cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate at least two kinds of information about the locations of the cellular telephones to which they provide service: (1) E-911 Phase II data, also known as GPS data or latitude-longitude data, and (2) cell-site data, also known as tower/face information or cell tower/sector record. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the cell

towers (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the sector (i.e., 120-degree face of the tower) to which the telephone connected during a call. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise than E-911 Phase II data.

8. Based on my training and experience, I know that Service Providers can collect E-911 Phase II data about the locations of the Subject Telephones by, inter alia, initiating a signal to determine the locations of the Subject Telephones on the Service Providers' networks or with such other reference points as may be reasonably available.

9. Based on my training and experience, I know that the Service Providers can collect cell-site data about the Subject Telephones.

AUTHORIZATION REQUEST

10. Based on the foregoing, I request that the Court issue the proposed search warrants, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c), 3103a and 3117. Federal Rule of Criminal Procedure 41(b)(4) provides that a magistrate judge may authorize the installation and use of a

tracking device within the meaning of 18 U.S.C. § 3117(b). See Rule 41(a)(2)(E). Section 3117(b) provides, in turn, that a "tracking device" is "an electronic or mechanical device which permits the tracking of the movement of a person or object." In addition, 18 U.S.C. § 3103a provides, in addition to the grounds for issuing a warrant under Rule 41, that "a warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States." Accordingly, this application seeks the E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information pursuant to Rule 41(e)(2)(C) and, to the extent that any of the information sought, such as the cell-site location data, constitutes a stored communication within the meaning of 18 U.S.C. § 2703, this application seeks the disclosure of that data pursuant to 18 U.S.C. §§ 2703(c) and 2711.

11. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrants to delay notice until 30 days after the collection authorized by the warrants has been completed. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrants may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the

subscribers or users of the Subject Telephones would seriously jeopardize the ongoing investigation, as such disclosure would give the targets of the investigation an opportunity to destroy evidence, harm or threaten victims or other witnesses, change patterns of behavior, notify confederates, and flee from and evade prosecution. Moreover, to the extent that the warrants authorize the seizure of any tangible property, any wire or electronic communication (as defined in 18 U.S.C. § 2510), or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above.

12. I further request that the Court direct the Service Providers to disclose to the government any information described in Attachment B that is within the Service Providers' possession, custody, or control. I also request that the Court direct the Service Providers to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Providers' services, by, inter alia, initiating a signal to determine the locations of the Subject Telephones on the Service Providers' networks or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The investigative agency shall

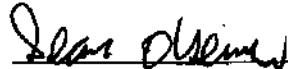
reasonably compensate the Service Providers for reasonable expenses incurred in furnishing such facilities or assistance.

13. I further request that the Court authorize execution of the warrants at any time of day or night, owing to the potential need to locate the Subject Telephones outside of daytime hours.

14. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation. Disclosure of this application and these orders would seriously jeopardize the ongoing investigation, as such a disclosure would give the targets of the investigation an opportunity to destroy

evidence, harm or threaten victims or other witnesses, change patterns of behavior, notify confederates and flee from or evade prosecution.

Dated: Brooklyn, New York
January 13, 2012


Sean Olsewski
Special Agent
Federal Bureau of Investigation

Sworn to before me the 13 day of January, 2012

s/R.E.R., Jr.

UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property To Be Searched

1. The cellular telephones assigned call numbers (A) (714) 348-6972, a cellular telephone subscribed to by "Doki Lungo" of the listed address "El Vido Way 45 23, Orange, CA" ("Subject Telephone #1"); and (B) (714) 253-2922, a prepaid cellular telephone with no subscriber information, but a listed address of 17330 Preston Road, Dallas, TX 75252 ("Subject Telephone #2") (collectively, the "Subject Telephones"), whose wireless telephone service providers are Sprint Nextel and AT&T, respectively (collectively, the "Service Providers").

2. Information about the location of the Subject Telephones that is within the possession, custody, or control of the Service Providers, including information about the location of the cellular telephone if it is subsequently assigned a different call number.

ATTACHMENT B

Particular Things to be Seized

All information about the location of the Subject Telephones described in Attachment A for a period of thirty (30) days, during all times of day and night. "Information about the location of the Subject Telephones" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which cell towers (i.e., antenna towers covering specific geographic areas) and sectors (i.e., 120-degree face of the towers) received radio signals from the Subject Telephones described in Attachment A.

To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Service Providers, the Service Providers are required to disclose the Location Information to the government. In addition, the Service Providers must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Service Providers' services, including by initiating a signal to determine the location of the Subject Telephones on the Service Providers' networks or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Providers for reasonable expenses incurred in furnishing such facilities or assistance.

To the extent that the Location Information includes tangible property, wire or electronic communications (as defined in 18 U.S.C. § 2510), or stored wire or electronic information, there is reasonable necessity for the seizure. See 18 U.S.C. § 3103a(b)(2).